[COMMITTEE PRINT]

JUNE 21, 1999

[Showing H.R. 850, As Approved by the Subcommittee on Telecommunications, Trade, and Consumer Protection]

106TH CONGRESS
1ST SESSION

H. R. 850

To amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 25, 1999

Mr. GOODLATTE (for himself, Ms. LOFGREN, Mr. ARMEY, Mr. DELAY, Mr. WATTS of Oklahoma, Mr. DAVIS of Virginia, Mr. COX, Ms. PRYCE of Ohio, Mr. BLUNT, Mr. GEPHARDT, Mr. BONIOR, Mr. FROST, Ms. DELAURO, Mr. LEWIS of Georgia, Mr. GEJDENSON, Mr. SENSENBRENNER, Mr. GEKAS, Mr. COBLE, Mr. SMITH of Texas, Mr. GALLEGLY, Mr. BRYANT, Mr. CHABOT, Mr. BARR of Georgia, Mr. HUTCHINSON, Mr. PEASE, Mr. CANNON, Mr. ROGAN, Mrs. BONO, Mr. BACHUS, Mr. CONYERS, Mr. FRANK of Massachusetts, Mr. BOUCHER, Mr. NADLER, Ms. JACKSON-LEE of Texas, Ms. WATERS, Mr. MEEHAN, Mr. DELAHUNT, Mr. WEXLER, Mr. ACKERMAN, Mr. ANDREWS, Mr. ARCHER, Mr. BALLENGER, Mr. BARCIA, Mr. BARRETT of Nebraska, Mr. BARRETT of Wisconsin, Mr. BARTON of Texas, Mr. BILBRAY, Mr. BLUMENAUER, Mr. BOEHNER, Mr. BRADY of Texas, Mr. BRADY of Pennsylvania, Ms. BROWN of Florida, Mr. BROWN of California, Mr. BURR of North Carolina, Mr. BURTON of Indiana, Mr. CAMP, Mr. CAMPBELL, Mrs. CAPPS, Mr. CHAMBLISS, Mrs. CHENOWETH, Mrs. CHRISTIAN-CHRISTENSEN, Mrs. CLAYTON, Mr. CLEMENT, Mr. CLYBURN, Mr. COLLINS, Mr. COOK, Mr. COOKSEY, Mrs. CUBIN, Mr. CUMMINGS, Mr. CUNNINGHAM, Mr. DAVIS of Illinois, Mr. DEAL of Georgia, Mr. DEFAZIO, Mr. DEUTSCH, Mr. DICKEY, Mr. DOOLEY of California, Mr. DOOLITTLE, Mr. DOYLE, Mr. DREIER, Mr. DUNCAN, Ms. DUNN, Mr. EHLERS, Mrs. EMERSON, Mr. ENGLISH, Ms. ESHOO, Mr. EWING, Mr. FARR of California, Mr. FIL-

NER, Mr. FORD, Mr. FOSSELLA, Mr. FRANKS of New Jersey, Mr. GILLMOR, Mr. GOODE, Mr. GOODLING, Mr. GORDON, Mr. GREEN of Texas, Mr. GUTKNECHT, Mr. HALL of Texas, Mr. HASTINGS of Washington, Mr. HERGER, Mr. HILL of Montana, Mr. HOBSON, Mr. HOEKSTRA, Mr. HOLDEN, Ms. HOOLEY of Oregon, Mr. HORN, Mr. HOUGHTON, Mr. INSLEE, Mr. ISTOOK, Mr. JACKSON of Illinois, Mr. JEFFERSON, Ms. EDDIE BERNICE JOHNSON of Texas, Mrs. JOHNSON of Connecticut, Mr. KANJORSKI, Mr. KASICH, Mrs. KELLY, Ms. KIKPATRICK, Mr. KIND, Mr. KINGSTON, Mr. KNOLLENBERG, Mr. KOLBE, Mr. LAMPSON, Mr. LARGENT, Mr. LATHAM, Ms. LEE, Mr. LEWIS of Kentucky, Mr. LINDER, Mr. LUCAS of Oklahoma, Mr. LUTHER, Ms. MCCARTHY of Missouri, Mr. MCDERMOTT, Mr. MCGOVERN, Mr. MCINTOSH, Mr. MALONEY of Connecticut, Mr. MANZULLO, Mr. MARKEY, Mr. MARTINEZ, Mr. MATSUI, Mrs. MEEK of Florida, Mr. METCALF, Mr. MICA, Ms. MILLENDER-MCDONALD, Mr. GEORGE MILLER of California, Mr. MOAKLEY, Mr. MORAN of Virginia, Mrs. MORELLA, Mrs. MYRICK, Mrs. NAPOLITANO, Mr. NEAL of Massachusetts, Mr. NETHERCUTT, Mr. NORWOOD, Mr. NUSSLE, Mr. OLVER, Mr. PACKARD, Mr. PALLONE, Mr. PASTOR, Mr. PETERSON of Minnesota, Mr. PICKERING, Mr. POMBO, Mr. POMEROY, Mr. PRICE of North Carolina, Mr. QUINN, Mr. RADANOVICH, Mr. RAHALL, Mr. RANGEL, Mr. REYNOLDS, Ms. RIVERS, Mr. ROHRABACHER, Ms. ROS-LEHTINEN, Mr. RUSH, Mr. SALMON, Ms. SANCHEZ, Mr. SANDERS, Mr. SANFORD, Mr. SCARBOROUGH, Mr. SCHAFFER, Mr. SESSIONS, Mr. SHAYS, Mr. SHERMAN, Mr. SHIMKUS, Mr. SMITH of Washington, Mr. SMITH of New Jersey, Mr. SOUDER, Ms. STABENOW, Mr. STARK, Mr. SUNUNU, Mr. TANNER, Mrs. TAUSCHER, Mr. TAUZIN, Mr. TAYLOR of North Carolina, Mr. THOMAS, Mr. THOMPSON of Mississippi, Mr. THUNE, Mr. TIAHRT, Mr. TIERNEY, Mr. UPTON, Mr. VENTO, Mr. WALSH, Mr. WAMP, Mr. WATKINS, Mr. WELLER, Mr. WHITFIELD, Mr. WICKER, Ms. WOOLSEY, and Mr. WU) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on International Relations, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

APRIL 27, 1999

Reported from the Committee on the Judiciary

APRIL 27, 1999

Referral to the Committee on International Relations extended for a period ending not later than July 2, 1999

APRIL 27, 1999

Referred to the Committees on Armed Services and Commerce and the Permanent Select Committee on Intelligence for a period ending not later than July 2, 1999

[Strike out all after the enacting clause and insert the part shown in roman.]

A BILL

To amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Security and Freedom through Encryption (SAFE) Act''.

SEC. 2. DEFINITIONS.

For purposes of this Act, the following definitions shall apply:

(1) COMPUTER HARDWARE.—The term ''computer hardware'' includes computer systems, equipment, application-specific assemblies, smart cards, modules, integrated circuits, printed circuit board assemblies, and devices that incorporate 1 or more microprocessor-based central processing units that are capable of accepting, storing, processing, or providing output of data.

(2) ENCRYPT AND ENCRYPTION.—The terms ''encrypt'' and ''encryption'' means the scrambling (and descrambling) of wire communications, electronic communications, or electronically stored infor-

mation, using mathematical formulas or algorithms to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information.

(3) ENCRYPTION PRODUCT.—The term ''encryption product''—

(A) means computer hardware, computer software, or technology with encryption capabilities; and

(B) includes any subsequent version of or update to an encryption product, if the encryption capabilities are not changed.

(4) KEY.—The term ''key'' means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire communications, electronic communications, or electronically stored information, that has been encrypted.

(5) KEY RECOVERY INFORMATION.—The term ''key recovery information'' means information that would enable obtaining the key of a user of encryption.

(6) PERSON.—The term ''person'' has the meaning given the term in section 2510 of title 18, United States Code.

(7) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce.

(8) STATE.—The term ''State'' means any State of the United States and includes the District of Columbia and any commonwealth, territory, or possessions of the United States.

(9) UNITED STATES PERSON.—The term ''United States person'' means any—

(A) United States citizen; or

(B) legal entity that—

(i) is organized under the laws of the United States, or any States, the District of Columbia, or any commonwealth, territory, or possession of the United States; and

(ii) has its principal place of business in the United States.

(10) WIRE COMMUNICATION; ELECTRONIC COMMUNICATION.—The terms ''wire communication'' and ''electronic communication'' have the meanings given such terms in section 2510 of title 18, United States Code.

SEC. 3. ENSURING DEVELOPMENT AND DEPLOYMENT OF ENCRYPTION IS A VOLUNTARY PRIVATE SECTOR ACTIVITY.

(a) STATEMENT OF POLICY.—It is the policy of the United States that the use, development, manufacture, sale, distribution, and importation of encryption products, standards, and services for purposes of assuring the confidentiality, authenticity, or integrity of electronic information shall be voluntary and market driven.

(b) LIMITATION ON REGULATION.—Neither the Federal Government nor a State may establish any conditions, ties, or links between encryption products, standards, and services used for confidentiality, and those used for authenticity or integrity purposes.

SEC. 4. PROTECTION OF DOMESTIC SALE AND USE OF ENCRYPTION.

Except as otherwise provided by this Act, it is lawful for any person within any State, and for any United States person in a foreign country, to develop, manufacture, sell, distribute, import, or use any encryption product, regardless of the encryption algorithm selected, encryption length chosen, existence of key recovery, or other plaintext access capability, or implementation or medium used.

SEC. 5. PROHIBITION ON MANDATORY GOVERNMENT ACCESS TO PLAINTEXT.

(a) IN GENERAL.—No department, agency, or instrumentality of the United States or of any State may require that, set standards for, condition any approval on, create incentives for, or tie any benefit to a requirement that, a decryption key, access to a key, key recovery information, or any other plaintext access capability be—

(1) required to be built into computer hardware or software for any purpose;

(2) given to any other person (including a department, agency, or instrumentality of the United States or an entity in the private sector that may be certified or approved by the United States or a State); or

(3) retained by the owner or user of an encryption key or any other person, other than for encryption products for the use of the United States Government or a State government.

(b) PROTECTION OF EXISTING ACCESS.—Subsection (a) does not affect the authority of any investigative or law enforcement officer, or any member of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), acting under any law in effect on the date of the enactment of this Act, to gain access to encrypted communications or information.

SEC. 6. UNLAWFUL USE OF ENCRYPTION IN FURTHERANCE OF A CRIMINAL ACT.

(a) ENCRYPTION OF INCRIMINATING COMMUNICATIONS OR INFORMATION UNLAWFUL.—Any person who, in the commission of a felony under a criminal statute of the United States, knowingly and willfully encrypts incriminating communications or information relating to that felony with the intent to conceal such communications or information for the purpose of avoiding detection by law enforcement agencies or prosecution—

(1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined under title 18, United States Code, or both; and

(2) in the case of a second or subsequent offense under this section, shall be imprisoned for not more than 10 years, or fined under title 18, United States Code, or both.

(b) USE OF ENCRYPTION NOT A BASIS FOR PROBABLE CAUSE.—The use of encryption by any person shall not be the sole basis for establishing probable cause with respect to a criminal offense or a search warrant.

SEC. 7. EXPORTS OF ENCRYPTION.

(a) AMENDMENT TO EXPORT ADMINISTRATION ACT OF 1979.—Section 17 of the Export Administration Act

of 1979 (50 U.S.C. App. 2416) is amended by adding at the end the following new subsection:

"(g) CERTAIN CONSUMER PRODUCTS, COMPUTERS, AND RELATED EQUIPMENT.—

"(1) GENERAL RULE.—Subject to paragraphs (2), (3), and (4), the Secretary shall have exclusive authority to control exports of all computer hardware, software, computing devices, customer premises equipment, communications network equipment, and technology for information security (including encryption), except that which is specifically designed or modified for military use, including command, control, and intelligence applications.

"(2) CRITICAL INFRASTRUCTURE PROTECTION PRODUCTS.—

"(A) IDENTIFICATION.—Not later than 90 days after the date of the enactment of the Security and Freedom through Encryption (SAFE) Act, the Assistant Secretary of Commerce for Communications and Information and the National Telecommunications and Information Administration shall issue regulations that identify, define, or determine which products and equipment described in paragraph (1) are

designed for improvement of network security, network reliability, or data security.

''(B) NTIA RESPONSIBILITY.—Not later than the expiration of the 2-year period beginning on the date of the enactment of the Security and Freedom through Encryption (SAFE) Act, all authority of the Secretary under this subsection and all determinations and reviews required by this section, with respect to products and equipment described in paragraph (1) that are designed for improvement of network security, network reliability, or data security through the use of encryption, shall be exercised through and made by the Assistant Secretary of Commerce for Communications and Information and the National Telecommunications and Information Administration. The Secretary may, at any time, assign to the Assistant Secretary and the NTIA authority of the Secretary under this section with respect to other products and equipment described in paragraph (1).

''(3) ITEMS NOT REQUIRING LICENSES.—After a one-time technical review by the Secretary of not more than 30 working days, no export license may be required, except pursuant to the Trading with the

Enemy Act or the International Emergency Economic Powers Act (but only to the extent that the authority of such Act is not exercised to extend controls imposed under this Act), for the export or reexport of—

"(A) any computer hardware or software or computing device, including computer hardware or software or computing devices with encryption capabilities—

"(i) that is generally available;

"(ii) that is in the public domain for which copyright or other protection is not available under title 17, United States Code, or that is available to the public because it is generally accessible to the interested public in any form; or

"(iii) that is used in a commercial, off-the-shelf, consumer product or any component or subassembly designed for use in such a consumer product available within the United States or abroad which—

"(I) includes encryption capabilities which are inaccessible to the end user; and

"(II) is not designed for military or intelligence end use;

"(B) any computing device solely because it incorporates or employs in any form—

"(i) computer hardware or software (including computer hardware or software with encryption capabilities) that is exempted from any requirement for a license under subparagraph (A); or

"(ii) computer hardware or software that is no more technically complex in its encryption capabilities than computer hardware or software that is exempted from any requirement for a license under subparagraph (A) but is not designed for installation by the purchaser;

"(C) any computer hardware or software or computing device solely on the basis that it incorporates or employs in any form interface mechanisms for interaction with other computer hardware or software or computing devices, including computer hardware and software and computing devices with encryption capabilities;

"(D) any computing or telecommunication device which incorporates or employs in any

form computer hardware or software encryption capabilities which—

"(i) are not directly available to the end user; or

"(ii) limit the encryption to be point-to-point from the user to a central communications point or link and does not enable end-to-end user encryption;

"(E) technical assistance and technical data used for the installation or maintenance of computer hardware or software or computing devices with encryption capabilities covered under this subsection; or

"(F) any encryption hardware or software or computing device not used for confidentiality purposes, such as authentication, integrity, electronic signatures, nonrepudiation, or copy protection.

"(4) COMPUTER HARDWARE OR SOFTWARE OR COMPUTING DEVICES WITH ENCRYPTION CAPABILITIES.—After a one-time technical review by the Secretary of not more than 30 working days, the Secretary shall authorize the export or reexport of computer hardware or software or computing devices

with encryption capabilities for nonmilitary end uses in any country—

"(A) to which exports of computer hardware or software or computing devices of comparable strength are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such computer hardware or software or computing devices will be—

"(i) diverted to a military end use or an end use supporting international terrorism;

"(ii) modified for military or terrorist end use;

"(iii) reexported without any authorization by the United States that may be required under this Act; or

"(iv)(I) harmful to United States national security, including United States capabilities in fighting drug trafficking, terrorism, or espionage, (II) used in illegal activities involving the sexual exploitation of, abuse of, or sexually explicit conduct with minors (including activities in violation of chapter 110 of title 18, United

States Code, and section 2423 of such title), or (III) used in illegal activities involving organized crime; or

"(B) if the Secretary determines that a computer hardware or software or computing device offering comparable security is commercially available outside the United States from a foreign supplier, without effective restrictions.

"(5) DEFINITIONS.—For purposes of this subsection—

"(A) the term 'computer hardware' has the meaning given such term in section 2 of the Security and Freedom through Encryption (SAFE) Act;

"(B) the term 'computing device' means a device which incorporates one or more microprocessor-based central processing units that can accept, store, process, or provide output of data;

"(C) the term 'customer premises equipment' means equipment employed on the premises of a person to originate, route, or terminate communications;

"(D) the term 'data security' means the protection, through techniques used by indi-

vidual computer and communications users, of data from unauthorized penetration, manipulation, or disclosure;

"(E) the term 'encryption' has the meaning given such term in section 2 of the Security and Freedom through Encryption (SAFE) Act;

"(F) the term 'generally available' means, in the case of computer hardware or computer software (including computer hardware or computer software with encryption capabilities)—

"(i) computer hardware or computer software that is—

"(I) distributed through the Internet;

"(II) offered for sale, license, or transfer to any person without restriction, whether or not for consideration, including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval;

"(III) preloaded on computer hardware or computing devices that

are widely available for sale to the public; or

''(IV) assembled from computer hardware or computer software components that are widely available for sale to the public;

''(ii) not designed, developed, or tailored by the manufacturer for specific purchasers or users, except that any such purchaser or user may—

''(I) supply certain installation parameters needed by the computer hardware or software to function properly with the computer system of the user or purchaser; or

''(II) select from among options contained in the computer hardware or computer software; and

''(iii) with respect to which the manufacturer of that computer hardware or computer software—

''(I) intended for the user or purchaser, including any licensee or transferee, to install the computer hardware or software and has sup-

plied the necessary instructions to do so, except that the manufacturer of the computer hardware or software, or any agent of such manufacturer, may also provide telephone or electronic mail help line services for installation, electronic transmission, or basic operations; and

''(II) the computer hardware or software is designed for such installation by the user or purchaser without further substantial support by the manufacturer;

''(F) the term 'network reliability' means the prevention, through techniques used by providers of computer and communications services, of the malfunction, and the promotion of the continued operations, of computer or communications network;

''(G) the term 'network security' means the prevention, through techniques used by providers of computer and communications services, of authorized penetration, manipulation, or disclosure of information of a computer or communications network;

''(H) the term 'technical assistance' includes instruction, skills training, working knowledge, consulting services, and the transfer of technical data;

''(I) the term 'technical data' includes blueprints, plans, diagrams, models, formulas, tables, engineering designs and specifications, and manuals and instructions written or recorded on other media or devices such as disks, tapes, or read-only memories; and

''(J) the term 'technical review' means a review by the Secretary of computer hardware or software or computing devices with encryption capabilities, based on information about the product's encryption capabilities supplied by the manufacturer, that the computer hardware or software or computing device works as represented.''.

(b) TRANSFER OF AUTHORITY TO NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION.—Section 103(b) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 902(b)) is amended by adding at the end the following new paragraph:

''(4) EXPORT OF COMMUNICATIONS TRANSACTION TECHNOLOGIES.—In accordance with section 17(g)(2) of the Export Administration Act of 1979 (50 U.S.C. App. 2416(g)(2)), the Secretary shall assign to the Assistant Secretary and the NTIA the authority of the Secretary under such section 17(g), with respect to products and equipment described in paragraph (1) of such section that are designed for improvement of network security, network reliability, or data security, that (after the expiration of the 2-year period beginning on the date of the enactment of the Security and Freedom through Encryption (SAFE) Act) is to be exercised by the Assistant Secretary and the NTIA.''.

(c) NO REINSTATEMENT OF EXPORT CONTROLS ON PREVIOUSLY DECONTROLLED PRODUCTS.—Any encryption product not requiring an export license as of the date of enactment of this Act, as a result of administrative decision or rulemaking, shall not require an export license on or after such date of enactment.

(d) APPLICABILITY OF CERTAIN EXPORT CONTROLS.—

(1) IN GENERAL.—Nothing in this Act shall limit the authority of the President under the International Emergency Economic Powers Act, the

Trading with the Enemy Act, or the Export Administration Act of 1979, to—

(A) prohibit the export of encryption products to countries that have been determined to repeatedly provide support for acts of international terrorism; or

(B) impose an embargo on exports to, and imports from, a specific country.

(2) SPECIFIC DENIALS.—The Secretary of Commerce may prohibit the export of specific encryption products to an individual or organization in a specific foreign country identified by the Secretary, if the Secretary determines that there is substantial evidence that such encryption products will be used for military or terrorist end-use.

(e) CONTINUATION OF EXPORT ADMINISTRATION ACT.—For purposes of carrying out the amendment made by subsection (a), the Export Administration Act of 1979 shall be deemed to be in effect.

SEC. 8. GOVERNMENT PROCUREMENT OF ENCRYPTION PRODUCTS.

(a) STATEMENT OF POLICY.—It is the policy of the United States—

(1) to permit the public to interact with government through commercial networks and infrastructure; and

(2) to protect the privacy and security of any electronic communication from, or stored information obtained from, the public.

(b) PURCHASE OF ENCRYPTION PRODUCTS BY FEDERAL GOVERNMENT.—Any department, agency, or instrumentality of the United States may purchase encryption products for internal use by officers and employees of the United States to the extent and in the manner authorized by law.

(c) PROHIBITION OF REQUIREMENT FOR CITIZENS TO PURCHASE SPECIFIED PRODUCTS.—No department, agency, or instrumentality of the United States, nor any department, agency, or political subdivision of a State, may require any person in the private sector to use any particular encryption product or methodology, including products with a decryption key, access to a key, key recovery information, or any other plaintext access capability, to communicate with, or transact business with, the government.

SEC. 9. NATIONAL ELECTRONIC TECHNOLOGIES CENTER.

Part A of the National Telecommunications and Information Administration Organization Act is amended by

inserting after section 105 (47 U.S.C. 904) the following new section:

"SEC. 106. NATIONAL ELECTRONIC TECHNOLOGIES CENTER.

"(a) ESTABLISHMENT.—There is established in the NTIA a National Electronic Technologies Center (in this section referred to as the 'NET Center').

"(b) DIRECTOR.—The NET Center shall have a Director, who shall be appointed by the Assistant Secretary.

"(c) DUTIES.—The duties of the NET Center shall be—

"(1) to serve as a center for industry and government entities to exchange information and methodology regarding data security techniques and technologies;

"(2) to examine encryption techniques and methods to facilitate the ability of law enforcement to gain efficient access to plaintext of communications and electronic information;

"(3) to conduct research to develop efficient methods, and improve the efficiency of existing methods, of accessing plaintext of communications and electronic information;

"(4) to investigate and research new and emerging techniques and technologies to facilitate

access to communications and electronic information, including —

"(A) reverse-steganography;

"(B) decompression of information that previously has been compressed for transmission; and

"(C) de-multiplexing;

"(5) to obtain information regarding the most current computer hardware and software, telecommunications, and other capabilities to understand how to access information transmitted across computer and communications networks; and

"(6) to serve as a center for Federal, State, and local law enforcement authorities for information and assistance regarding decryption and other access requirements.

"(d) EQUAL ACCESS.—State and local law enforcement agencies and authorities shall have access to information, services, resources, and assistance provided by the NET Center to the same extent that Federal law enforcement agencies and authorities have such access.

"(e) PERSONNEL.—The Director may appoint such personnel as the Director considers appropriate to carry out the duties of the NET Center.

''(f) ASSISTANCE OF OTHER FEDERAL AGENCIES.—Upon the request of the Director of the NET Center, the head of any department or agency of the Federal Government may, to assist the NET Center in carrying out its duties under this section—

''(1) detail, on a reimbursable basis, any of the personnel of such department or agency to the NET Center; and

''(2) provide to the NET Center facilities, information, and other non-personnel resources.

''(g) PRIVATE INDUSTRY ASSISTANCE.—The NET Center may accept, use, and dispose of gifts, bequests, or devises of money, services, or property, both real and personal, for the purpose of aiding or facilitating the work of the Center. Gifts, bequests, or devises of money and proceeds from sales of other property received as gifts, bequests, or devises shall be deposited in the Treasury and shall be available for disbursement upon order of the Director of the NET Center.

''(h) ADVISORY BOARD.—

''(1) ESTABLISHMENT.—There is established the Advisory Board of the NET Center (in this subsection referred to as the ''Advisory Board''), which shall be comprised of 11 members who shall have the qualifications described in paragraph (2) and

who shall be appointed by the Assistant Secretary not later than 6 months after the date of the enactment of this Act. The chairman of the Advisory Board shall be designated by the Assistant Secretary at the time of appointment.

''(2) QUALIFICATIONS.—Each member of the Advisory Board shall have experience or expertise in the field of encryption, decryption, electronic communication, information security, electronic commerce, or law enforcement.

''(3) DUTIES.—The duty of the Advisory Board shall be to advise the NET Center and the Federal Government regarding new and emerging technologies relating to encryption and decryption of communications and electronic information.

''(i) IMPLEMENTATION PLAN.—Within 2 months after the date of the enactment of this Act, the Assistant Secretary, in consultation and cooperation with other appropriate Federal agencies and appropriate industry participants, develop and cause to be published in the Federal Register a plan for establishing the NET Center. The plan shall—

''(1) specify the physical location of the NET Center and the equipment, software, and personnel

resources necessary to carry out the duties of the NET Center under this section;

''(2) assess the amount of funding necessary to establish and operate the NET Center; and

''(3) identify sources of probable funding for the NET Center, including any sources of in-kind contributions from private industry.''.

SEC. 10. STUDY OF NETWORK AND DATA SECURITY ISSUES.

Part C of the National Telecommunications and Information Administration Organization Act is amended by adding at the end the following new section:

''SEC. 156. STUDY OF NETWORK RELIABILITY AND SECURITY AND DATA SECURITY ISSUES.

''(a) IN GENERAL.—The NTIA shall conduct an examination of—

''(1) the relationship between—

''(A) network reliability (for communications and computer networks), network security (for such networks), and data security issues; and

''(B) the conduct, in interstate commerce, of electronic commerce transactions, including through the medium of the telecommunications networks, the Internet, or other interactive computer systems;

''(2) the availability of various methods for encrypting communications; and

''(3) the effects of various methods of providing access to encrypted communications and to information to further law enforcement activities.

''(b) SPECIFIC ISSUES.—In conducting the examination required by subsection (a), the NTIA shall—

''(1) analyze and evaluate the requirements under paragraphs (3) and (4) of section 17(g) of the Export Administration Act of 1979 (50 U.S.C. App. 2416(g); as added by section 7(a) of this Act) for products referred to in such paragraphs to qualify for the license exemption or mandatory export authorization under such paragraphs, and determine—

''(A) the scope and applicability of such requirements and the products that, at the time of the examination, qualify for such license exemption or export authorization; and

''(B) the products that will, 12 months after the examination is conducted, qualify for such license exemption or export authorization; and

''(2) assess possible methods for providing access to encrypted communications and to information to further law enforcement activities.

''(c) REPORTS.—Within one year after the date of enactment of this section, the NTIA shall submit to the Congress and the President a detailed report on the examination required by subsections (a) and (b). Annually thereafter, the NTIA shall submit to the Congress and the President an update on such report.

''(d) DEFINITIONS.—For purposes of this section—

''(1) the terms 'data security', 'encryption', 'network reliability', and 'network security' have the meanings given such terms in section 17(g)(5) of the Export Administration Act of 1979 (50 U.S.C. App. 2416(g)(5)); and

''(2) the terms 'Internet' and 'interactive computer systems' have the meanings provided by section 230(e) of the Communications Act of 1934 (47 U.S.C. 230(e)).

SEC. 11. TREATMENT OF ENCRYPTION IN INTERSTATE AND FOREIGN COMMERCE.

(a) INQUIRY REGARDING IMPEDIMENTS TO COMMERCE.—Within 180 days after the date of the enactment of this Act, the Secretary of Commerce shall complete an inquiry to—

(1) identify any domestic and foreign impediments to trade in encryption products and services and the manners in which and extent to which such

impediments inhibit the development of interstate and foreign commerce; and

(2) identify import restrictions imposed by foreign nations that constitute trade barriers to providers of encryption products or services.

The Secretary shall submit a report to the Congress regarding the results of such inquiry by such date.

(b) REMOVAL OF IMPEDIMENTS TO TRADE.—Within 1 year after such date of enactment, the Secretary shall prescribe such regulations as may be necessary to reduce the impediments to trade in encryption products and services identified in the inquiry pursuant to subsection (a) for the purpose of facilitating the development of interstate and foreign commerce. Such regulations shall be designed to—

(1) promote the sale and distribution, including through electronic commerce, in foreign commerce of encryption products and services manufactured in the United States; and

(2) strengthen the competitiveness of domestic providers of encryption products and services in foreign commerce, including electronic commerce.

(c) INTERNATIONAL AGREEMENTS.—

(1) REPORT TO PRESIDENT.—Upon the completion of the inquiry under subsection (a), the Sec-

retary shall submit a report to the President regarding reducing any impediments to trade in encryption products and services that are identified by the inquiry and could, in the determination of the Secretary, require international negotiations for such reduction.

(2) NEGOTIATIONS.—The President shall take all actions necessary to conduct negotiations with other countries for the purposes of (A) concluding international agreements on the promotion of encryption products and services, and (B) achieving mutual recognition of countries' export controls, in order to meet the needs of countries to preserve national security, safeguard privacy, and prevent commercial espionage. The President may consider a country's refusal to negotiate such international export and mutual recognition agreements when considering the participation of the United States in any cooperation or assistance program with that country. The President shall submit a report to the Congress regarding the status of international efforts regarding cryptography not later than December 31, 2000.

SEC. 12. COLLECTION OF INFORMATION ON EFFECT OF ENCRYPTION ON LAW ENFORCEMENT ACTIVITIES.

(a) COLLECTION OF INFORMATION BY ATTORNEY GENERAL.—The Attorney General shall compile, and maintain in classified form, data on the instances in which encryption (as defined in section 2801 of title 18, United States Code) has interfered with, impeded, or obstructed the ability of the Department of Justice to enforce the criminal laws of the United States.

(b) AVAILABILITY OF INFORMATION TO THE CONGRESS.—The information compiled under subsection (a), including an unclassified summary thereof, shall be made available, upon request, to any Member of Congress.